

The invention claimed is:

1 1. (Original) A method for producing a shortened representation of a collection of
2 bits, comprising the steps of:
3 inputting the collection of “n” bits;
4 summing a key having at least “n” bits with the collection of bits to produce a
5 sum;
6 squaring the sum to produce a squared sum;
7 performing a modular “p” operation on the squared sum, where “p” is at least as
8 large as a first prime number greater than 2^n to produce a modular “p” result;
9 performing a modular 2^l operation on the modular “p” result to produce a
10 modular 2^l result where, “l” is less than “n”; and
11 outputting the modular 2^l result.

1 2. (Original) A method for producing a shortened representation of a collection of
2 bits, comprising the steps of:
3 inputting the collection of “n” bits;
4 summing a first key having at least “n” bits with the collection of bits to produce a
5 first sum;
6 squaring the first sum to produce a squared sum;
7 summing the squared sum with a second key having at least “n” bits to produce a
8 second sum;
9 performing a modular “p” operation on the second sum, where “p” is at least as
10 large as a first prime number greater than 2^n to produce a modular “p” result;
11 performing a modular 2^l operation on the modular “p” result to produce a
12 modular 2^l result where, “l” is less than “n”; and
13 outputting the modular 2^l result.

1 3. (Original) A method for producing a shortened representation of a collection of
2 bits, comprising the steps of:
3 inputting a collection of “n” bits;

4 summing a key having at least “n” bits with the collection of bits to produce a
5 sum;
6 squaring the sum to produce a squared sum;
7 repeating the previous three steps at least once to produce a plurality of squared
8 sums, where a different key is used each time the steps are repeated;
9 summing the plurality of squared sums to produce a summation;
10 performing a modular “p” operation on the summation, where “p” is at least as
11 large as a first prime number greater than 2^n to produce a modular “p” result;
12 performing a modular 2^l operation on the modular “p” result to produce a
13 modular 2^l result where, “l” is less than “n”; and
14 outputting the modular 2^l result.